



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,400	12/08/2003	Tsz Simon Cheng	BOC9-2003-0073 (444)	4573
40987	7590	08/19/2008		
AKERMAN SENTERFITT P. O. BOX 3188 WEST PALM BEACH, FL 33402-3188			EXAMINER WANG, HARRIS C	
			ART UNIT	PAPER NUMBER
			2139	
			MAIL DATE	DELIVERY MODE
			08/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/730,400	Applicant(s) CHENG ET AL.	
	Examiner HARRIS C. WANG	Art Unit 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 May 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 and 20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18, 20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to claims 1-18, 20 have been considered but are moot in view of the new ground(s) of rejection.

Claim 19 has been cancelled.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-18, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese (20030217137) in view of Baird (20030115481) in view of Wright, further in view of Barch.

Regarding Claims 1, 6-7, 12-13, 18

Roese teaches a method for managing the display of sensitive content in non-trusted environments, comprising the steps of:

interrogating a list of policies associated with a given user and a physical device

(Fig. 4, Is User Authenticated to Access Requested Information?, Step 425);

determining a location of the physical device; *(Fig. 4, Identify Location of Device Associated with Querying User, Step 415)*

comparing the location of the physical device with a list of trusted locations;

("With the received location information, system 100 authenticates that the physical location of the client device is in a permitted and authorized location for access to the requested network resources" Paragraph [106])

and enforcing a plurality of rules for managing the presentation of sensitive content contained in the policy, wherein access to sensitive information is limited or restricted based on the location *("If system 100 determines that the location is not verified, system denies access or restricts access according to predefined policies (e.g. deny any access or restrict access to only those devices...available to the general public" Paragraph [0111])*

Roese teaches providing access to a service that maintains an organization list of individuals and machine identification information indicating that a listed individual or machine is associated with a predetermined organization (*"system 100 provides another example of a location-aware network and is described as an enterprise network that serves as a data communication network for a business organization or other type of enterprise"* Paragraph [0132]); determining that an individual or machine on the list is within a predetermined proximity of the physical device, and in response thereto, transmitting a physical alert to the physical device (*"secure military and intelligence environment can require that certain physical locations be protected from unauthorized use of computing systems available in that secure location...When a user tries to authenticate, the authentication/location server employs the location of the user requesting authorization when validating credentials...If the user fails to meet the security level associated that particular location, then the network...sounds alarms and/or reports the location of the unauthorized user"* Paragraph [0104]) The Examiner interprets the individual on a list is a user that lacks the proper security level.

Roese does not explicitly teach wherein the service is subscription based.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the service be subscription based.

The motivation is that many services are subscription based and one of ordinary skill in the art would be able to modify the service of Roese to be a subscription based service with predictable results.

While Roesse does teach limiting access based on location (*Paragraph [0097-99], Figures 4-6*), Roesse does not explicitly teach blocking a visual presentation or audible presentation of at least one object in portions of the presentation, wherein the step of enforcing comprises at least one of blacking out a visual object in a display during the presentation, replacing a visual object with innocuous content during the presentation, visually hiding the at least one object from the given user during the presentation and inserting audio “white noise” gaps in an audio object, if a physical device is not located in a trusted location.

Baird teaches blocking the visual display of at least one object in portions of the presentation, wherein the step of enforcing comprises blacking out a visual object in a display during the presentation. (*Figure 3, “The Server determines whether the source of the request is authorized to receive a complete version of the requested document” Step 310, “Redact the unauthorized portions of the document” Step 316, “Transmit the redacted version of the document to the source of the request” 318*)

It is well known that redaction is defined as editing or blacking out text in a document or to the result of such an effort. It is intended to allow the selective disclosure of information in a document while keeping other parts of the document secret. (See Wikipedia)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the location sensitive access method of Roesse with the well known method of redacting parts of a document as taught by Baird.

The motivation to combine is that both Baird teaches a well known method of redacting sensitive content if a requestor is not authorized, and Roese teaches denying or restricting access if the requestor is not authorized. One of ordinary skill would be able to modify Roese to redact sensitive content as a way of restricting access.

Roese and Baird do not further teaching that the list of policies are corporate policies, where the policy data is acquired locally from the physical device or dynamically via access to a corporate network, each corporate policy prohibiting or restricting access to corporate data in a non-trusted environment.

Wright (20040123150) teaches a location based security system wherein the policies are corporate policies, each corporate policy prohibiting or restricting access to corporate data in a nontrusted environment. (*"In another example the location detection module determines whether the mobile device is operating in the "work" location network environment" Paragraph [0078]*)(*"The policy for the "software lab" environment allows a mobile device accessing a corporate server to access certain files while a mobile device trying to access the files via the conference room NAP receives a notification that these files cannot be found" Paragraph [0080]*)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the location based security policies of Roese and Baird to include corporate policies prohibiting or restricting access to corporate data in a nontrusted environment as taught by Wright.

The motivation is to “protect against unwanted access to information stored on mobile devices and corporate servers (Paragraph [0004] of Wright)”

Roese Baird and Wright do not explicitly teach upon determining that an individual or machine is associated with a competitive organization transmitting an alert to the physical device

Karch (7140035) teaches a policy where an individual associated with a competitive organization is prevented from accessing corporate data (“an analyst consulting for a specific company must be prevented from accessing information about companies that are competitive with that company” Column 4, lines 7-9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the security policy as taught in the previous references to preclude an individual associated with a competitive organization as taught by Karch.

The motivation is to prevent “a conflict of interest” (Column 4, lines 6-7 of Karch)

Roese teaches a system which inherently has a memory and a processor. Roese further teaches a GPS as part of the system (*Paragraph [106]*), GPS units inherently have displays.

Roese teaches a machine-readable storage, having stored thereon a computer program having a plurality of code sections (*“System 100 employs both hardware and software (e.g. an application executing on server 134) to provide location-aware services*

described below. Paragraph [0028]) executable by a machine for causing the machine to method as described

Regarding Claim 2, 8, 14

Roese, Baird, Wright and Barch further teach providing a reminder of the policy regarding confidential material to the given user in response to an attempt to access sensitive information on the physical device. (*“when a device seeks network access from a location deemed not to be inherently secure, system 100 can prompt a user to initiate an improved connection...or can inform the user that supplemental restrictions apply while in the insecure area. More generally, this can be seen as an expansion of policy based access”* Paragraph [0114] of Roese)

The Examiner interprets the informing the user that supplemental restrictions apply as a reminder of the policy regarding confidential material.

Roese teaches a system which inherently has a memory and a processor. Roese further teaches a GPS as part of the system (*Paragraph [106]*), GPS units inherently have displays.

Roese teaches a machine-readable storage, having stored thereon a computer program having a plurality of code sections (*“System 100 employs both hardware and software (e.g. an application executing on server 134) to provide location-aware services*

described below. Paragraph [0028]) executable by a machine for causing the machine to method as described

Regarding Claim 3-4, 9-10, 15-16

Roesse, Baird, Wright and Karch further teach the step of requesting authentication from the given user in response to an attempt to access sensitive information in an open application on the physical device, wherein the step of requesting authentication comprises at least one among requesting provision of a unique password for the given user, a unique accessing device, or a unique biometric characteristic of the given user. (*"a user seeking access to system 100 can first be authenticated...system 100 achieves this portion of the authorization process by requiring the end user at a location client device to supply certain user information...including one or more passwords"* Paragraph [0105], Roesse)

Roesse teaches that the steps of authentication may be repeated while the device is connected to the network, which the Examiner interprets as "an open application." (*"this process, and other processes involving determining or verifying device locations that are described below, may be repeated while the device is connected to the network for any of a number of reason of interest to the network admin that re-determining is required"* Paragraph [0077])

Roesse teaches a system which inherently has a memory and a processor. Roesse further teaches a GPS as part of the system (*Paragraph [106]*), GPS units inherently have displays.

Roesse teaches a machine-readable storage, having stored thereon a computer program having a plurality of code sections (*"System 100 employs both hardware and software (e.g. an application executing on server 134) to provide location-aware services described below. Paragraph [0028]"*) executable by a machine for causing the machine to method as described

Regarding Claim 5, 11, 17

Roesse, Baird, Wright and Barch further teach the step of determining a location comprises the step of using at least one among a global positioning system and a terrestrial wireless infrastructure system to provide the location of the physical device. (*"In one example. System 100 permits requested access from devices having pre-approved location identifying equipment...this can include a GPS receiver" Paragraph [106], Roesse*)

Roesse teaches a system which inherently has a memory and a processor. Roesse further teaches a GPS as part of the system (*Paragraph [106]*), GPS units inherently have displays.

Roesse teaches a machine-readable storage, having stored thereon a computer program having a plurality of code sections (*"System 100 employs both hardware and software (e.g. an application executing on server 134) to provide location-aware services*

described below. Paragraph [0028]) executable by a machine for causing the machine to method as described

Regarding Claim 19

Roese, Baird, Wright and Karch further teach presenting an alert when a competitor listed in a profile is within a proximity of the location. (*"The expanded location database may contain, for example, attributes such as..."minimal security level...If the user has a security clearance of a high enough level to authenticate from that location, the authentication process proceeds. If the user fails to meet the security level associated...the network can halt the authentication process, sound alarms and/or report the location of the unauthorized user"* Paragraph [0104-0105] Roese) The Examiner interprets the competitor as the unauthorized user in the proximity of the location database, wherein the alert sounds while the competitor is within the location.

Regarding Claim 20,

Roese, Baird, Wright and Barch further teach identifying a seniority level of the given user; and granting a permission to override the policy based on the seniority. (*"The expanded location database may contain, for example, attributes such as..."minimal security level...If the user has a security clearance of a high enough level to authenticate from that location, the authentication process proceeds. If the user fails to meet the security level*

associated...the network can halt the authentication process, sound alarms and/or report the location of the unauthorized user” Paragraph [0104-0105 of Reese)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KRISTINE KINCAID can be reached on (571) 272-4063. The fax phone

Art Unit: 2139

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139